Attorney's Docket No.: 5220.P002 Patent

In re the Application of: Dave Parker, et al. **APPELLANT'S BRIEF UNDER 37 C.F.R. § 1.192**
(inventor(s))

Application No.: 09/703,329

Filed: October 31, 2000

For: METHOD OF AND APPARATUS FOR NETWORK ADMINISTRATION
(title)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

SIR: Transmitted herewith is an **Appellant's Brief Under 37 C.F.R. § 1.192** for the above application.

__X__ **Reply Brief Under 37 C.F.R. § 1.192** is enclosed.
_____ A check for $0.00 is attached for processing fees under 37 C.F.R. § 1.17 (f).
_____ A check in the amount of $_____ is attached for presentation of additional claim(s).
_____ Applicant(s) hereby Petition(s) for an Extension of Time of _____ month(s) pursuant to 37 C.F.R. § 1.136(a).
_____ A check for _____ is attached for processing fees under 37 C.F.R. § 1.136 (a).
_____ Please charge my Deposit Account No. 02-2666 the amount of $_____.
A duplicate copy of this sheet is enclosed.
X_____ The Commissioner of Patents and Trademarks is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 02-2666 **(a duplicate copy of this sheet is enclosed)**:
__X__ Any additional filing fees required under 37 C.F.R. § 1.16 for presentation of extra claims.
__X__ Any extension or petition fees under 37 C.F.R. § 1.17.

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date: November 19, 2007

Daniel E. Ovanezian

Reg. No. 41,236

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

FIRST CLASS CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, PO Box 1450, Alexandria, Virginia 22313-1450.

on 11/19/07 Judy L. Steinkraus
Date of Deposit Name of Person Mailing Correspondence

Signature 11/19/2007
Date

Attorney Docket No: 5220.P002

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Examiner: Alam, Uzma
Dave Parker et al.	Art Unit: 2157
Application No.: 09/703,329	Confirmation Number: 3235
Filed: October 31, 2000	
For: METHOD OF AND APPARATUS FOR NETWORK ADMINISTRATION	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. § 1.192, Appellants submit the following Reply Brief for consideration by the Board of Patent Appeals and Interferences (hereinafter "Board"). Please charge any amounts due or credit any overpayment to Deposit Account No. 02-2666.

FIRST CLASS CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, V.A. 22313-1450

on 11/19/07 Judy L. Steinkraus
Date

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the full interest of the invention, Red Hat, Inc., of 1801 Varsity Drive, Raleigh, NC, 27606.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

Claims 1-7, 9-14, 16-18, 20-24, 26-28, 30-33, 42-43, 45-46 and 48 are currently pending in the above-referenced application. Claims 1-7, 9-14, 16-18, 20-24, 26-28, 30-33, 42-43, 45-46 and 48 were rejected in the Final Office Action mailed on December 29, 2006, and are presented for appeal. Claims 8, 15, 19, 25, 29, 34-37, 44 and 47 are canceled. Claims 38-41 are withdrawn from consideration. A copy of claims 1-48 as they stand on appeal are set forth in Appendix A.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Embodiments of the instant application relate to network administration. Administrating a network may include operations such as monitoring, notification and reporting of a status of a business site's infrastructures. The monitoring may capture

pertinent health and status information of hosts using a satellite system. This information may be used for reports that the business site may generate about the hosts. (See Abstract).

In an exemplary implementation of independent claim 1, a method includes accessing a port of a host system and logging into the host system by a satellite system to monitor an internal parameter for a predetermined event related to the host system. (Specification, page 14, lines 16-19; page 25, lines 12-15; Figure 7, block 710). Data about the predetermined event is transferred from the satellite system to a monitoring operations center (MOC). (Specification, page 16, lines 9-10; page 25, lines 15-16; Figure 7, block 720). The monitoring operations center (MOC) generates a notification upon an occurrence of the predetermined event to a first person in a hierarchy. (Specification, page 25, lines 16-20; Figure 7, block 730). When the first person fails to acknowledge the notification in a time period, the MOC escalates the notification to a second person in the hierarchy. (Specification, page 26, lines 1-6; Figure 7, block 750).

In an exemplary implementation of independent claim 7, a method includes monitoring a host system for a parameter corresponding to a predetermined event using a satellite system located locally to the host system. (Specification, page 9, lines 7-10; page 25, lines 12-15; Figure 7, block 710). Data about the predetermined event collected by the satellite system is queued. (Specification, page 16, lines 9-16). Queuing the data includes queuing different types of data in different ones of multiple queues. (Specification, page 16, lines 9-16). A transfer of the queued data from the multiple queues is prioritized. (Specification, page 16, lines 14-16). The queued data is transferred from the host system to a monitoring operations center (MOC).

(Specification, page 16, lines 9-10; page 25, lines 15-16; Figure 7, block 720). The MOC is located externally from the host system, and generates a notification to a first person in a hierarchy upon an occurrence of the predetermined event. (Specification, page 8, lines 2-6; page 25, lines 16-20; Figure 7, block 730). When the first person fails to acknowledge the notification in a time period, the MOC escalates the notification to a second person in the hierarchy. (Specification, page 26, lines 1-6; Figure 7, block 750).

In an exemplary implementation of independent claim 20, a machine readable medium has stored thereon instructions, which when executed by a processor, cause the processor to perform the actions described below. A monitoring operations center (MOC) receives data about an occurrence of a predetermined event related to a host system. (Specification, page 25, lines 15-16; Figure 7, block 720). The occurrence of the predetermined event is determined by access of a port of the host system by a satellite system. (Specification, page 13, lines 12-15; page 14, lines 16-19). The monitoring operations center (MOC) generates a notification upon an occurrence of the predetermined event to a first person in a hierarchy. (Specification, page 25, lines 16-20; Figure 7, block 730). When the first person fails to acknowledge the notification in a time period, the MOC escalates the notification to a second person in the hierarchy. (Specification, page 26, lines 1-6; Figure 7, block 750). At least one of a suggestion of a probable cause of the predetermined event and a solution to the occurrence of the predetermined event is provided. (Specification, page 22, lines 12-18).

In an exemplary implementation of independent claim 26, an apparatus includes a means for logging into and monitoring a host system for an internal parameter corresponding to a predetermined event. (Specification, page 12, lines 7-14, page 12

line 20 to page 13, line 11, page 14, lines 17-19; Figure 3, blocks 325 and 326). Internal monitoring may include recording of states over time, identification of state changes, and notification of state changes. (Specification, page 14, line 17 to page 15, line 7). The apparatus includes a means for generating a notification upon the occurrence of the predetermined event to a first person in a hierarchy. The means may include a notification server and/or a notification gateway. (Specification, page 15, lines 3-5, page 19, line 14 to page 21, line 2, page 10, lines 13-16; Figure 3, block 300; Figure 5, blocks 570 and 580). The apparatus includes a means for escalating the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period. (Specification, page 21, line 3 to page 22, line 2).

In an exemplary implementation of independent claim 30, an apparatus includes a configuration portal to interface with a satellite system over a communication link and configure a service interleave factor of a host system. (Specification, page 16, lines 17-19, page 18, lines 1-17, page 25, lines 4-11; Figure 5, block 590). The service interleave factor determines how service checks are interleaved. (Specification, page 18, lines 1-17). The apparatus includes a digital processing system coupled to the portal, the digital processing system to receive data indicative of an occurrence of the event and generate a first notification. (Specification, page 10, line 17 to page 18, line 6, page 17, lines 2-8; Figure 3, block 300). The apparatus includes a notification gateway coupled to the digital processing system to transmit the first notification to a first communication device. (Specification, page 19, lines 17 to page 20, line 14; Figure 5, block 580). The digital processing system generates a second notification to a

second communication device if an acknowledgement is not received within a predetermined time. (Specification, page 21, lines 3-11).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues involved in this Appeal are as follows:

A. Whether claims 1-7, 9-14, 16-18, 20-24, 26-28, 30-33, 42-43 and 45-48 are anticipated by U.S. Publication No. 2001/0044840 to Carleton et al. ("Carleton").

VII. ARGUMENT

A. Claims 1-7, 9-14, 16-18, 20-24, 26-28, 30-33, 42-43 and 45-48 are not anticipated by U.S. Publication No. 2001/0044840 to Carleton et al. ("Carleton") because Carleton fails to disclose each of the elements of these claims.

1. Claim 1 and associated dependent claims 2-6, 9-14, 16-18, 42 and 46 are not anticipated by Carleton because Carleton fails to disclose logging into a host system by a satellite system to monitor an internal parameter for a predetermined event related to the host system.

Appellants respectfully submit that Carleton does not disclose logging into a host system by a satellite system to monitor an internal parameter of the host.

Carleton discloses a network monitor that collects status and statistics about device operation in a client network, and transmits the status and statistics to a monitoring server. (Carleton, page 3, paragraph [0050]). All status and statistics collected by the network monitor of Carleton are based on port information, and can be collected by pinging or polling networked computers. (See Carleton, paragraph [0054], lines 4-8, paragraph [0075], lines 1-25, paragraph [0087], lines 1-4, paragraph [0092], lines 1-6). Such port information includes ping related information such as ping response (Carleton, paragraph [0075], lines 5-6), ping status (Carleton, paragraph [0075], lines 23-25), port activity (Carleton, paragraph [0075], lines 15-17), and an interval of broken communication (Carleton, paragraph [0054], lines 4-8). All of these status and statistics are **parameters that exist external to a host system**.

In the Office Action of December 29, 2006, the Examiner stated:

> Carleton teaches that a client server [22] collects status and statistics about device operation in the client network. The client server 22 is connected to various client devices 26a-26c and 32a-32c. The client server transmits this information to the monitoring and administration system 20. The alarms generated for a device are about the device itself and all the ports associated with the device, as taught in paragraph 0075. Specific device (26a-26c) information, such as level of port activity, are monitored by the system. These are internal parameters of the host system.

(Office Action, 12, 29, 2006, page 11).

The appellants respectfully disagree with the Examiner's conclusion that the parameters monitored by the system are internal parameters. All of the parameters described by the Examiner are **external** parameters. The present application describes external parameters, stating, "[f]or external monitoring, host satellite system 250 monitors network services of a host by accessing the host's ports that are connected to the intranetwork 215." (Current Application, Page 13, lines 12-15). As described in the current application, parameters monitored merely by accessing a host's ports are external parameters. Since the parameters that are monitored by Carleton are all parameters that are gathered merely by accessing a host's ports, Carleton discloses monitoring only external parameters. In contrast, claim 1 discloses monitoring an internal parameter.

Moreover, Carleton does not disclose a satellite system logging into a host system, as required by claim 1. In Carleton, there is no need to log into the host system, because internal parameters of the host system are not monitored. Accordingly, Carleton does not even suggest a system logging into the host system. In the Office Action of October 4, 2006, the Examiner stated that "Carleton **does not** teach

that the system logs into the device." (Office Action, 08/04/2006, page 11). In contrast, claim 1 discloses logging into a host system by a satellite system.

In the Office Action of December 29, 2006, the Examiner asserted that Carleton **does** teach the system logging into the device, stating:

> The systems are connected to the devices via the network (pp 0049, lines 17-19 and pp 0050, lines 1-3). Information is required about the users which are to be allowed to access system information concerning the network being monitored (pp 0058). Each prospective user is required to log into the system prior to gaining access to the network information (pp0058). Once the user logs on to the system, that user has access to all the regions and devices on the network that it is allowed to access (pp0060). See also pp0092.

(Office Action, 12/29/2006, page 11).

The appellants respectfully disagree with the Examiner's conclusion that Carleton discloses a satellite system logging into a host system, and submit that the Examiner's statements supporting such a conclusion are inapposite. The examiner has described a section of Carleton entitled, "User Information," in which Carleton discloses how a user logs into a remote network monitoring and administration system to access network information that has been gathered, or to change user preferences or permissions. (Carleton, paragraphs [0057]-[0060]). The Examiner is confusing a user logging into an administration system, as described in Carleton, with a satellite system logging into a host system, as recited in claim 1. In Carleton, the user is an individual (e.g., an administrator, service user, or system operator). (Carleton, paragraph [0059], lines 17-19). The user disclosed in Carleton is not a satellite system. Therefore, Carleton does not disclose a satellite system logging into a host system, as required by claim 1.

In the Examiner's Answer, the Examiner attempted to clarify his argument that Carleton teaches a satellite system logging into a host system, stating:

> With respect to the claims, the client system is the host system, the client server is the satellite server. The internal parameters being monitored are the status of devices, paragraphs 0084-0087. The invention claims logging into a host system by a satellite system to monitor an internal parameter. Carleton teaches logging into a satellite system to gain access to a host system and all the status and information about the system (paragraphs 0048 and 0059). ... Each prospective user is required to log into the [satellite] system prior to gaining access to the network information. (paragraph 0058). Once the user logs on to the system, that user had access to all the regions and devices on the network that it is allowed to access (paragraph 0060). See also Figure 4, paragraph 0092.

(Examiner's Answer, 09/18/2007, pages 13-14).

Examiner continues to confuse a user logging into an administration system, as described in Carleton, with a satellite system logging into a host system, as recited in claim 1. If, as the Examiner suggests, the client system of Carleton is the host system of claim 1, and the client server of Carleton is the satellite server of Claim 1, then to support Examiner's assertions, Carleton must at least disclose the client server logging into the client system. However, Carleton *does not* disclose the client server logging into the client system. Instead, Carleton teaches a *user* 40 logging into an *administration system* 20. (See Figure 1). As discussed above, a user logging into an administration system is not the same as a satellite system logging into a host system. Moreover, the user 40 is logging into the administration system 20 to monitor external parameters of *a remote network* 12. (Carleton, paragraph [0050]). In contrast, claim 1 recites logging into a host system by a satellite system to monitor an internal parameter for a predetermined event *related to the host system.*

Carleton does not disclose monitoring internal parameters, nor does Carleton disclose a satellite system logging into a host system. Therefore, Carleton does not disclose logging into a host system by a satellite system to monitor an internal parameter for a predetermined event related to the host system, as required by claim 1. Accordingly, independent claim 1 and dependent claims 2-6, 9-14, 16-18, 42 and 46 are not anticipated by Carleton.

2. Claim 7 and associated dependent claim 43 are not anticipated by Carleton because Carleton fails to disclose queuing different types of data in different ones of multiple queues or prioritizing a transferring of queued data from multiple queues.

Carleton does not disclose queuing different types of data in different ones of multiple queues. Moreover, Carleton does not even disclose the use of queues, much less queuing different types of data in different queues, or prioritizing a transferring of queued data from multiple queues.

In the Office Action of December 29, 2006, the Examiner stated:

> On page 16 of the specification of the claimed invention, the Applicant discloses that queues are used to store and queue different types of data. Paragraph 0075 of the reference Carleton teaches that the monitoring device receives information about current alarms in devices. In Carleton different alarms are coded differently to generate a variety of reports, each report relating to a specific alarm. Carleton teaches that one device is monitored for different business rules. See paragraph 0075. The reference also teaches that a variety of reports are generated. See paragraph 0087. A number of additional reports exist within the system and custom reports may be created so that the administrator is supplied with the information required to properly administer the system. The custom reports allow the administrator to manage, transfer and manipulate

> data that comes in from different ports on the host into different lists. Storing and generating different types of data based on different alarms teaches the queue of the claimed invention.

(Office Action, 12/29/2006, pages 11-12).

The appellants respectfully disagree with the Examiner's statement that Carleton discloses using queues, and submit that the analysis provided by the Examiner is inapposite.

First, the Examiner points to a discussion of queues in the specification of the present application as evidence that Carleton discloses queues. It appears that the Examiner is improperly resorting to the specification of the present invention to define the terms and disclosure of the cited Carleton reference. It is submitted that such an action is improper. Specifically, the MPEP states that "[w]hen a U.S. patent, a U.S. patent application publication, or an international application publication is used to reject claims under 35 U.S.C. 102(e), the disclosure relied on in the rejection must be present in the issued patent or application publication. (MPEP, 2136.02(II), 2100-93). Therefore, it is submitted that the Examiner must look to what is described in the Carleton reference, itself, for determining the disclosure of Carleton.

The paragraphs relied upon by the Examiner as disclosing the use of different ones of multiple queues describe monitoring a device for different business rules and generating a variety of reports for the device. (Carleton, paragraphs [0075], [0084], [0086] and [0087]). However, neither monitoring a device for different business rules, nor generating a variety of reports for the device, are the same as queuing different types of data in different ones of multiple queues. Monitoring a device for different business rules consists of pinging a port of a device, and applying business rules (e.g.,

notify rules) based on a result. (Carleton, paragraph [0072], lines 10-14) and paragraph [0075], lines 1-9). Generating reports consists of displaying current and/or past system information based on region, device zone, or individual devices. (Carleton, paragraphs [0084]-[0087]). Neither the discussion of the monitoring nor the reporting includes a disclosure of the use of multiple queues.

For the sake of argument, even if the monitoring of business rules and generation of reports were interpreted to include the use of different ones of multiple queues, Carlton still fails to disclose prioritizing a transferring of queued data from the multiple queues. The Examiner stated that paragraph [0075] of Carleton discloses such prioritizing of multiple queues. Paragraph [0075] is reproduced below:

> The current alarm status screen of FIG. 12 opens when the link "view current alarms" is selected from the home page. The alarm status screen for a device within the system preferably comprises a port selection grid, device information, device alarms, and ping related information, such as ping response graphs from the device. The current status is delivered in real-time by the system so that the user or administrator can monitor actual status and keep updated on changes. The user may select a port number within the grid at the top of FIG. 12, numbered from "01" to "60" to select a port for which additional information is desired. Upon selecting a port, the graphs of FIG. 13 are displayed. The graphs are "InOctet" and "OutOctet" traffic graphs for the particular port. The graphs preferably span an interval of a month (upper graph), and a year (lower graph). The graphs depict the level of port activity over the span of time specified. Referring again to FIG.12, if any current alarms exist within a device, they are displayed in a block of "current alarms" which provide information about the specific alarm. The port number generating the alarm is specified in a "port" field and the send time of the most recent notification on the alarm is provided in a "last alerted" field. A "ping status" field indicates if the selected device is responding to pings. An "admin status" field indicates how the device is configured comprising the states of "up", "down", "test", "NA" (not applicable). An "OP status" field denotes if the device is responding to the SNMP agent, with the possible states being given as "up", "down", "test", or "NA". A "level" field indicates the escalation level for the alarm, while a "status" field displays the current status of the device, such as "alarm", "cleartime", and "acknowledge."

(Carleton, paragraph [0075]).

As shown, nowhere in paragraph [0075] does Carleton disclose prioritizing multiple queues. Nor does Carleton disclose such a limitation elsewhere. Accordingly, Carleton fails to disclose either queuing different types of data in different ones of multiple queues or prioritizing a transferring of queued data from multiple queues. Therefore, independent claim 7 and dependent claim 43 are not anticipated by Carleton.

3. Claim 20 and associated dependent claims 21-24 and 45 are not anticipated by Carleton because Carleton fails to disclose providing at least one of a suggestion of a probable cause of a predetermined event and a solution to the occurrence of the predetermined event.

Carleton does not disclose providing a probable cause of a predetermined event or a solution to the occurrence of the predetermined event, as required by claim 20.

In the Office Action of December 29, 2006, the Examiner stated that, "[i]n paragraph 0087 [*sic*], the reference Carleton teaches that the cause of the alarm is indicated in the report generated by the monitoring system (pp0084, line 12-16). (Office Action, 12/29/2006, page 12). Paragraph [0084] is reproduced below:

> The monitoring and administration system allows viewing of system information and provides variously formatted reports of status and history within the system. Accessible upon login are a "view device by region" screen as exemplified by FIG. 21 and a "view device by zone" screen as exemplified by FIG. 22. Each of these screens, which are shown having at least one section expanded, provide a hierarchical view of the respective regions or zones which contain devices defined within the system. Entries within the tree are preferably highlighted in colors to indicate alarm status within the respective zone or region. In FIG. 21, both "Lincoln plaza" and "remote offices" are highlighted to indicate that alarm

> conditions exist within those regions. In FIG. 22 the headline "printers" and the specific device "printer 207.212.77.224" are highlighted to indicate the cause of the current printer alarm. Preferably, the alarm indication at a hierarchical level, such as "printers" is distinguishable from the indication used for a device, such as "printer 207.212.77.224" by highlighting in a different color. The described embodiment denotes alarm categories by yellow highlighting and specific devices as pink highlighting.

(Carleton, paragraph [0084]).

The Examiner has confused a probable cause of a predetermined event with a cause of an alarm. In Carleton, the predetermined event (e.g., a business rule violation) is the cause of the alarm (e.g., failure of a specific printer). In contrast, the cause of the predetermined event would disclose why the predetermined event was invoked (e.g., what caused the printer to fail). The reports disclosed by Carleton do not provide a probable cause of the predetermined event. The reports of Carleton indicate only the cause of an alarm, which indicates the device that is the source, or point of origin, of the alarm. In contrast, the probable cause of a predetermined event, as recited by claim 20, indicates the reason or explanation of fact as to why a particular device has had a predetermined event. Therefore, Carleton does not disclose providing at least one of a suggestion of a probable cause of the predetermined event and a solution to the occurrence of the predetermined event, and thus does not have all of the limitations of claim 20. Accordingly, independent claim 20 and dependent claims 21-24 and 45 are not anticipated by Carleton.

4. Claim 26 and associated dependent claims 27-28 are not anticipated by Carleton because Carleton fails to disclose a means for logging into and monitoring a host system for an internal parameter.

Appellants respectfully submit that Carleton does not disclose a means for logging into and monitoring a host system for an internal parameter.

Carleton discloses a network monitor that collects status and statistics about device operation in a client network, and transmits the status and statistics to a monitoring server. (Carleton, page 3, paragraph [0050]). All status and statistics collected by the network monitor of Carleton are based on port information, and can be collected by pinging or polling networked computers. (See Carleton, paragraph [0054], lines 4-8, paragraph [0075], lines 1-25, paragraph [0087], lines 1-4, paragraph [0092], lines 1-6). Such port information includes ping related information such as ping response (Carleton, paragraph [0075], lines 5-6), ping status (Carleton, paragraph [0075], lines 23-25), port activity (Carleton, paragraph [0075], lines 15-17), and an interval of broken communication (Carleton, paragraph [0054], lines 4-8). All of these status and statistics are **parameters that exist external to a host system**.

In the Office Action of December 29, 2006, the Examiner stated:

> Carleton teaches that a client server [22] collects status and statistics about device operation in the client network. The client server 22 is connected to various client devices 26a-26c and 32a-32c. The client server transmits this information to the monitoring and administration system 20. The alarms generated for a device are about the device itself and all the ports associated with the device, as taught in paragraph 0075. Specific device (26a-26c) information, such as level of port activity, are monitored by the system. These are internal parameters of the host system.

(Office Action, 12, 29, 2006, page 11).

The appellants respectfully disagree with the Examiner's conclusion that Carleton discloses a system that monitors internal parameters. All of the parameters described by the Examiner are **external** parameters. The present application describes external parameters, stating, "[f]or external monitoring, host satellite system 250 monitors network services of a host by accessing the host's ports that are connected to the intranetwork 215." (Current Application, Page 13, lines 12-15). As described in the current application, parameters monitored merely by accessing a host's ports are external parameters. Since the parameters that are monitored by Carleton are all parameters that are gathered merely by accessing a host's ports, Carleton discloses monitoring only external parameters. In contrast, claim 26 discloses a means for monitoring an internal parameter.

Moreover, Carleton does not disclose a means for logging into a host system, as required by claim 26. In Carleton, there is no need to log into the host system, because internal parameters of the host system are not monitored. Accordingly, Carleton does not even suggest a system logging into the host system. In the Office Action of October 4, 2006, the Examiner stated that "Carleton **does not** teach that the system logs into the device." (Office Action, 08/04/2006, page 11). In contrast, claim 26 discloses a means for logging into a host system.

In the Office Action of December 29, 2006, the Examiner asserted that Carleton **does** teach the system logging into the device, stating:

> The systems are connected to the devices via the network (pp 0049, lines 17-19 and pp 0050, lines 1-3). Information is required about the users which are to be allowed to access system information concerning the network being monitored (pp 0058). Each prospective user is required to log into the system prior to gaining access to the network information

(pp0058). Once the user logs on to the system, that user has access to all the regions and devices on the network that it is allowed to access (pp0060). See also pp0092.

(Office Action, 12/29/2006, page 11).

The appellants respectfully disagree with the Examiner's conclusion that Carleton discloses a means for logging into a host system, and submit that the Examiner's statements supporting such a conclusion are inapposite. The examiner has described a section of Carleton entitled, "User Information," in which Carleton discloses how a user logs into a remote network monitoring and administration system to access network information that has been gathered, or to change user preferences or permissions. (Carleton, paragraphs [0057]-[0060]). The Examiner is confusing a user logging into an administration system, as described in Carleton, with an apparatus that includes a means for logging into a host system, as recited in claim 26. In Carleton, the user is an individual (e.g., an administrator, service user, or system operator). (Carleton, paragraph [0059], lines 17-19). The user disclosed in Carleton is not a means of an apparatus that logs into a host system. Therefore, Carleton does not disclose a means for logging into a host system, as required by claim 26.

In the Examiner's Answer, the Examiner attempted to clarify his argument that Carleton teaches a satellite system logging into a host system, stating:

With respect to the claims, the client system is the host system, the client server is the satellite server. The internal parameters being monitored are the status of devices, paragraphs 0084-0087. The invention claims logging into a host system by a satellite system to monitor an internal parameter. Carleton teaches logging into a satellite system to gain access to a host system and all the status and information about the system (paragraphs 0048 and 0059). ... Each prospective user is required to log into the [satellite] system prior to gaining access to the network information. (paragraph 0058).

> Once the user logs on to the system, that user had access to all the regions and devices on the network that it is allowed to access (paragraph 0060). See also Figure 4, paragraph 0092.

(Examiner's Answer, 09/18/2007, pages 13-14).

Examiner continues to confuse a user logging into an administration system, as described in Carleton, with a satellite system logging into a host system, as recited in claim 26. If, as the Examiner suggests, the client system of Carleton is the host system of claim 26, and the client server of Carleton is the satellite server of Claim 26, then to support Examiner's assertions, Carleton must at least disclose the client server logging into the client system. However, Carleton *does not* disclose the client server logging into the client system. Instead, Carleton teaches a *user* 40 logging into an *administration system* 20. (See Figure 1). As discussed above, a user logging into an administration system is not the same as a satellite system logging into a host system.

Carleton does not disclose a means for monitoring internal parameters, nor does Carleton disclose a means for logging into a host system. Therefore, Carleton does not disclose a means for logging into and monitoring a host system for an internal parameter, as required by claim 26. Accordingly, independent claim 26 and dependent claims 27-28 are not anticipated by Carleton.

5. Claim 30 and associated dependent claims 31-33 and 48 are not anticipated by Carleton because Carleton fails to disclose configuring a service interleave factor of a host system.

Carleton does not disclose interleaving, an interleave factor, or any terms that are synonymous to interleaving or an interleave factor.

The Office Action of December 29, 2006 states:

> Interleaving, as understood by the Examiner, is arranging data in alternating portions. In Carleton, checks are performed on devices based on certain business rules. Some of these checks are done at only specific times. See paragraphs 0062, 0072, 0073. Only alarms which relate to a certain rule are evaluated. Because not all ports and all rules are being monitored at all times, Carleton teaches interleave factors.

(Office Action, 12/29/2006, page 12).

Appellants respectfully disagree with the conclusion that Carleton discloses interleaving, and submit that the Examiner's analysis is inapposite. A disclosure in Carleton that checks are performed on devices based on business rules is not a disclosure of interleaving. Nor does an evaluation of alarms that relate to a certain rule, or monitoring of less than all ports and all rules at all times equate to a disclosure of interleaving. The Examiner is erroneously reading additional limitations into the disclosure of Carleton. The Office Actions have cited paragraphs [0051], [0054], [0062]-[0073], [0075], and [0087] as disclosing interleave factors. However, none of these paragraphs indicate the use of interleave factors. Nor is an interleave factor disclosed elsewhere in Carleton.

In the Examiner's Answer, the Examiner further stated:

Interleaving as defined in the specification is disclosed on page 18 as a more even distribution of service checks, reduced load on hosts and faster overall detection of host problems. Service interleave factor determines how checks are interleaved. On page 19, it is disclosed that intercheck delay determines how service checks are initially distributed in an event queue. The use of delays between service checks may help reduce, or even eliminate, CPU load spikes on a host. The specification also discloses on page 19, lines 4-6, that other types of parameters may be configured, for example, timing parameters. The timing parameters may include time between failed checks, check period and scheduling passes.

In Carleton, checks are performed on devices based on certain business rules. These rules or parameters specify when a device or port is polled for information. Some of these checks are done at only specific times. See paragraphs 0072, 0073. Also taught by Carleton in paragraph 0072, page 5, lines 1-5, is that different timing rules are set to poll a device. These rules include polling period, retries, timeout and backoff.

Carleton teaches configuring business rules to adhere to certain timing conditions. These conditions allow for a system or device to have some downtime. Accordingly, Carleton teaches configuring system interleave factors.

(Examiner's Answer, 9/18/2007, pages 19-20).

Applicants respectfully disagree with Examiner's conclusion that the timing rules disclosed in Carleton are the same as a service interleave factor. The specification of the present invention discloses multiple service parameters. Examples of such service parameters include service interleave factors (as claimed), maximum concurrent service checks, host check, inter-check delay, and timing parameters (e.g., time between failed checks, check period, and scheduling passes). Examiner has attempted to combine the features of many of the disclosed service parameters into the claimed service interleave factor. Specifically, Examiner discusses timing parameters and intercheck delays as if they were aspects of a service interleave factor. However, each of the service parameters described in the specification are **different parameters**. Therefore,

discussion of intercheck delay and timing parameters is inapposite, and it is incorrect to combine these features with those of the service interleave factor.

Of the described parameters, applicants have explicitly claimed the service interleave factor in claim 30. Therefore, to support Examiner's assertions, Carleton must at least disclose a service interleave factor. Carleton fails to disclose such a service interleave factor, or any parameters that are the same as a service interleave factor. As described by the Examiner, the business rules of Carleton can include specific timing rules, which consist of polling period, retries, timeout and backoff. These timing rules determine when a *specific* business rule will trigger. In contrast, a service interleave factor can determine how *multiple different checks* are applied, thus providing an even distribution of service checks. Therefore, timing rules as disclosed in Carleton are not the same as a service interleave factor.

Nowhere does Carleton disclose a service interleave factor. Accordingly, independent claim 30 and dependent claims 31-33 and 48 are not anticipated by Carleton.

VIII. CONCLUSION

Based on the foregoing, Appellants respectfully submit that the Board should reverse the rejections of all pending claims and hold that all of the claims currently under review are allowable.

Respectfully submitted,

Dated: 11/19, 2007

Daniel E. Ovanezian
Reg. No. 41,236

Customer No. 008791

IX. CLAIMS APPENDIX

The claims involved in this appeal are presented below.

1. (Currently Amended) A method, comprising:

accessing a port of a host system and logging into said host system by a satellite system to monitor an internal parameter for a predetermined event related to the host system;

transferring data about the predetermined event from the satellite system to a monitoring operations center;

generating, by the monitoring operations center, a notification upon an occurrence of the predetermined event to a first person in a hierarchy; and

escalating, by the monitoring operations center, the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period.

2. (Original) The method of claim 1, further comprising determining whether the notification is successful.

3. (Previously Presented) The method of claim 1, wherein the predetermined event is receipt of a state change of the internal parameter.

4. (Previously Presented) The method of claim 1, wherein the predetermined event is exceeding a threshold value set for the internal parameter.

5. (Original) The method of claim 1, further comprising generating the notification a number of times for an amount of time.

6. (Original) The method of claim 5, wherein the number of times, the amount of time, and the time period are configurable.

7. (Previously Presented) A method, comprising:

monitoring a host system for a parameter corresponding to a predetermined event using a satellite system located locally to the host system;

queuing data about the predetermined event collected by the satellite system, wherein queuing the data comprises queuing different types of the data in different ones of multiple queues;

prioritizing a transferring of the queued data from the multiple queues;

transferring the queued data from the host system to a monitoring operations center;

generating, by the monitoring operations center located remotely from the host system, a notification upon an occurrence of the predetermined event to a first person in a hierarchy; and

escalating, by the monitoring operations center, the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period.

8. (Canceled)

9. (Original) The method of claim 1, further comprising providing a possible cause of the predetermined event occurrence.

10. (Original) The method of claim 1, where escalation is based on a set of rules.

11. (Original) The method of claim 10, wherein the set of rules is based on a time delay between the notification and the acknowledgement.

12. (Original) The method of claim 10, wherein the set of rules is based on the state change.

13. (Original) The method of claim 10, wherein the set of rules is based on schedules of the first and second persons.

14. (Original) The method of claim 1, wherein the notification is generated and escalated automatically.

15. (Canceled)

16. (Previously Presented) The method of claim 1, further comprising monitoring a service of the host system by the satellite system.

17. (Original) The method of claim 1, wherein the parameter is a utilization of a component of the host system.

18. (Original) The method of claim 17, further comprising:

monitoring additional parameters of the host system, wherein the additional parameters include a service of the host system; and

eliminating a redundant notification based on dependent parameters of the host system.

19. (Canceled)

20. (Previously Presented) A machine readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform the following:

receiving, by a monitoring operations center data about an occurrence of a predetermined event related to a host system, the occurrence of the predetermined event determined by access of a port of the host system by a satellite system;

generating, by the monitoring operations center, a notification upon the occurrence of the predetermined event to a first person in a hierarchy;

escalating, by the monitoring operations center, the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period; and

providing at least one of a suggestion of a probable cause of the predetermined event and a solution to the occurrence of the predetermined event.

21. (Previously Presented) The machine readable medium of claim 20, wherein the predetermined event is receipt of a state change of the parameter.

22. (Previously Presented) The machine readable medium of claim 20, wherein the processor further performs generating the notification a number of times for an amount of time.

23. (Previously Presented) The machine readable medium of claim 20, wherein the number of times, the amount of time, and the time period are configurable.

24. (Previously Presented) The machine readable medium of claim 20, wherein the processor further performs providing a suggestion as to a cause of the predetermined event occurrence.

25. (Canceled)

26. (Currently Amended) An apparatus, comprising:

means for logging into and monitoring a host system for an internal parameter corresponding to a predetermined event;

means for generating a notification upon the occurrence of the predetermined event to a first person in a hierarchy; and

means for escalating the notification to a second person in the hierarchy when the first person fails to acknowledge the notification in a time period.

27. (Original) The apparatus of claim 26, further comprises means for determining whether the notification is successful.

28. (Original) The apparatus of claims 26, further comprising:

means for generating the notification a number of times for an amount of time.

29. (Canceled)

30. (Previously Presented) An apparatus, comprising:

a configuration portal to interface with a satellite system over a communication link and configure a service interleave factor of a host system, wherein the service interleave factor determines how service checks are interleaved;

a digital processing system coupled to the portal, the digital processing system to receive data indicative of an occurrence of the event and generate a first notification; and

a notification gateway coupled to the digital processing system to transmit the first notification to a first communication device, the digital processing system to

generate a second notification to a second communication device if an acknowledgment is not received within a predetermined time.

31. (Original) The apparatus of claim 30, wherein the notification gateway transmits the second notification to the second communication device.

32. (Original) The apparatus of claim 30, wherein the digital processing system comprises at least one server.

33. (Original) The apparatus of claim 30, further comprising a proxy server coupled to the digital processing system.

Claims 34.-37. (Canceled)

Claims 38.-41. (Not Entered).

42. (Previously Presented) The method of claim 1, wherein generating further comprises transmitting the occurrence of the predetermined event from the satellite system to the monitoring operations center.

43. (Previously Presented) The method of claim 7, wherein the parameter of the host system is monitored by a satellite system, and wherein generating further

comprises transmitting the occurrence of the predetermined event from the satellite system to the monitoring operations center to generate the notification.

44. (Canceled)

45. (Previously Presented) The method of claim 20, wherein generating further comprises transmitting the occurrence of the predetermined event from the satellite system to the monitoring operations center.

46. (Previously Presented) The method of claim 1, wherein accessing the port of the host system to monitor the internal parameter comprises logging into the host system.

47. (Canceled)

48. (Previously Presented) The apparatus of claim 30, wherein the service interleave factor determines how a plurality of service checks are interleaved.

X. EVIDENCE APPENDIX

No other evidence is submitted in connection with this appeal.

XI. RELATED PROCEEDINGS APPENDIX

No related proceedings exist.